Closed-Form Expressions for Secrecy Capacity over Correlated Rayleigh Fading Channels

Xiaojun Sun, Chunming Zhao, *Member IEEE,* and Ming Jiang, *Member IEEE,*

***Abstract*—We investigate the secure communications over correlated wiretap Rayleigh fading channels assuming the full channel state information (CSI) available. Based on the information theoretic formulation, we derive closed-form expressions for the average secrecy capacity and the outage probability. Simulation results confirm our analytical expressions.**

***Index Terms*—Information-theoretic security, wiretap channel, secrecy capacity, correlated Rayleigh fading.**

I. Introduction

Because wireless communications are susceptible to eavesdropping, traditional security mechanisms mainly rely on cryptographic protocols. Recently, potential benefits of deriving secure information from physical layer have been reported in [1]. In [2], the information-theoretic secrecy capacity was introduced by using the physical properties of channels.

The basic principle of information-theoretic security has been widely accepted as the strictest notion of security, which guarantees that the sent massages can not be decoded by a malicious eavesdropper [1]. Wyner introduced wiretap channel model to evaluate secure transmissions at the physical layer [2], where Alice transmits confidential data to Bob and Eve eavesdrops the data. Csiszar *et. al.* and Leung-Yan-Cheong *et. al.* generalized it to broadcast channels and basic Gaussian channels, respectively in [3] and [4]. Wei Kang *et. al.* studied secure communications over two-user semi-deterministic broadcast channels [5]. The secrecy capacity is defined as the difference between the main channel capacity (Alice to Bob) and the eavesdropping's channel capacity (Alice to Eve) [4]. Barros *et. al.* and Gopala *et. al.* generalized this Gaussian wiretap channel model to wireless quasi-static fading channels [6]-[8]. The secure MIMO systems are studied in [9]-[10]. Motivated by emerging wireless applications, there is a growing interest in exploiting the benefits of relay and cooperative strategies in order to guarantee secure transmissions [11]-[13].

In this paper, we consider the secure communications within Wyner's correlated wiretap channel by building on the detailed technique in [7]. Similar work studied in [14] gives the limiting value of the average secrecy capacity, which only converges into the secrecy capacity at the high signal-to-noise ratio (SNR). We derive the closed-form expressions of the average secure communication capacity and the outage probability under the assumption of the full channel state information (CSI) available. Simulation results verify our analytical expressions.

National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, CHINA. E-mail: {sunxiaojun, cmzhao, jiang_ming}@seu.edu.cn

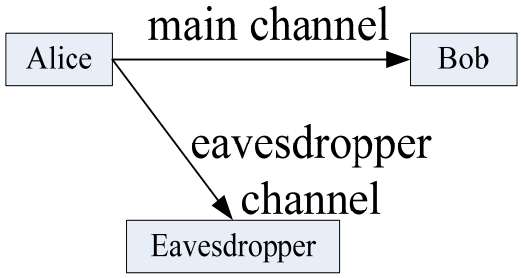

Fig. 1. Fading wiretap channel model.

II. System Model

Fig. 1 shows a fading wiretap channel model considered in this paper. Here, the source Alice transmits confidential information to the destination Bob. A third party (Eve) is able of eavesdropping on the transmissions. The received signals at Bob and Eve are given by

$$y = h_{sd}x + n_d \tag{1a}$$

$$z = h_{se}x + n_e \tag{1b}$$

where h_{se} and h_{sd} are complex Gaussian random variables (RV) with zero-mean. N_d and N_e denote zero-mean complex Gaussian noise RVs with unit-variance. The instantaneous SNRs $\alpha = |h_{sd}|^2$ and $\beta = |h_{se}|^2$ are exponentially distributed. The average value is λ_1 and λ_2, respectively.

Since α and β are correlated variables, the joint PDF is expressed as [14][15]

$$f(\alpha,\beta) = \frac{I_0\left(\frac{2}{1-\rho}\sqrt{\frac{\alpha\beta\rho}{\lambda_1\lambda_2}}\right)}{(1-\rho)\lambda_1\lambda_2}\exp\left(-\frac{\alpha/\lambda_1+\beta/\lambda_2}{1-\rho}\right) \tag{2}$$

where ρ is the correlation between h_{se} and h_{sd}. $I_0(\cdot)$ is the zeroth-order modified Bessel function of the first kind. Using the infinite-series representation of $I_0(x)$ [16]

$$I_0(x) = 1 + \sum_{k=1}^{\infty}\frac{x^{2k}}{4^k(k!)^2}$$

We can rewrite the joint PDF as

$$\begin{aligned} f(\alpha,\beta) &= \sum_{k=0}^{\infty} c_k \frac{\exp\left(-\frac{\alpha/\lambda_1+\beta/\lambda_2}{1-\rho}\right)}{\lambda_1\lambda_2}\left(\frac{\alpha}{\lambda_1}\right)^k\left(\frac{\beta}{\lambda_2}\right)^k \\ &= \sum_{k=0}^{\infty} c_k \frac{1}{\lambda_1\lambda_2}\exp\left(-\frac{\alpha/\lambda_1+\beta/\lambda_2}{1-\rho}\right)\left(\frac{\alpha}{\lambda_1}\right)^k\left(\frac{\beta}{\lambda_2}\right)^k \\ &= \sum_{k=0}^{\infty} c_k f_k(\alpha,\beta) \end{aligned} \tag{3}$$

where $c_k = \frac{\rho^k}{(k!)^2(1-\rho)^{2k+1}}$.

In this study, we assume that Alice has access to CSI on both the main channel and the eavesdropper's channel. For instance, Eve may be not a covert eavesdropper, but simply another user [6][7]. Alice wants to transmit some confidential data to Bob which Alice does not wish Eve know. So, Alice can estimate the CSI of the eavesdropper's channel [6][7].

III. Secure communications over correlated Rayleigh fading channel

Start with the technique detailed in [7], which introduces the secrecy capacity over fading channel. A similar introduction was presented in [8]. Recalling the results of [7] for the Rayleigh fading wiretap channel, the secrecy capacity for one realization can be written as

$$C_s(\alpha,\beta) = \begin{cases} \ln(1+\alpha) - \ln(1+\beta) \ , & if \ \ \alpha > \beta \\ 0 \qquad\qquad\qquad\quad , & if \ \ \alpha \leqslant \beta \end{cases} \tag{4}$$

where $\ln(1+\alpha)$ is the rate of the main channel, and $\ln(1+\beta)$ denotes the rate of the eavesdropper's channel.

A. average secrecy capacity

The average secrecy capacity over correlated channels is derived as follows.

Theorem 1: The average secrecy capacity is averaged over all channel realizations

$$\begin{aligned} \mathrm{C}_s &= \int_0^\infty \int_0^\infty C_s(\alpha,\beta) f(\alpha,\beta) d\alpha d\beta \\ &= \sum_{k=0}^{\infty} c_k k! (1-\rho)^{k+1} F\left(\lambda_1, k, \frac{1}{1-\rho}\right) \\ &-k! \sum_{m=0}^{k} \frac{(\lambda_1/\lambda_2)^m}{m!} (1-\rho)^{k+1-m} F\left(\lambda_1, k+m, \frac{1+\lambda_1/\lambda_2}{1-\rho}\right) \\ &-k! \sum_{m=0}^{k} \frac{(\lambda_2/\lambda_1)^m}{m!} (1-\rho)^{k+1-m} F\left(\lambda_2, k+m, \frac{1+\lambda_2/\lambda_1}{1-\rho}\right) \end{aligned} \tag{5}$$

where function $F(\lambda,k,\mu)$ can be recursively evaluated or computed by using popular symbolic software like MATLAB. After integration by parts, we get

$$\begin{aligned} F(\lambda,k,\mu) &= \int_0^\infty \ln(1+\lambda x) \exp(-\mu x) x^k dx \\ &= \frac{\lambda}{\mu} F_k + \frac{k}{\mu} F(\lambda, k-1, \mu) \end{aligned} \tag{6}$$

where F_k is defined by [16, 3.353.5]

$$\begin{aligned} F_k &= \int_0^\infty \frac{x^k}{1+\lambda x} e^{-\mu x} dx \\ &= \frac{1}{\lambda}\left[\left(-\frac{1}{\lambda}\right)^k \exp\left(\frac{\mu}{\lambda}\right) \mathrm{E}_1\left(\frac{\mu}{\lambda}\right) + \sum_{m=1}^{k} \Gamma(m) \frac{(-\lambda)^{m-k}}{\mu^m}\right]. \end{aligned}$$

Function $F(\lambda,0,\mu) = \frac{1}{\mu} E_1\left(\frac{\mu}{\lambda}\right) \exp\left(\frac{\mu}{\lambda}\right)$. $E_1(x) = \int_1^\infty \frac{e^{-xt}}{t} dt$ is the exponential-integral function [16]. $\Gamma(\cdot)$ is the gamma function [16].

Proof: The integral in (5) is re-expressed as

$$\begin{aligned} \mathrm{C}_s &= \sum_{k=0}^{\infty} c_k \int_0^\infty \int_0^\alpha \ln(1+\alpha) f_k(\alpha,\beta) d\alpha d\beta \\ &- \int_0^\infty \int_\beta^\infty \ln(1+\beta) f_k(\alpha,\beta) d\alpha d\beta \\ &= \sum_{k=0}^{\infty} c_k \int_0^\infty \int_0^{\lambda_1 u/\lambda_2} \ln(1+\lambda_1 u) f_k(u,v) du dv \\ &- \int_0^\infty \int_{\lambda_2 v/\lambda_1}^\infty \ln(1+\lambda_2 v) f_k(u,v) du dv \\ &= \sum_{k=0}^{\infty} c_k \left(R_k^1 - R_k^2\right) \end{aligned}$$

The integral R_k^1 can be evaluated by[16, 3.381.1]

$$\begin{aligned} R_k^1 &= \int_0^\infty \ln(1+\lambda_1 u) \exp\left(-\frac{u}{1-\rho}\right) u^k du \\ &\times \int_0^{\lambda_1 u/\lambda_2} \exp\left(-\frac{v}{1-\rho}\right) v^k dv \\ &= \int_0^\infty (1-\rho)^{k+1} \ln(1+\lambda_1 u) \exp\left(-\frac{u}{1-\rho}\right) u^k \\ &\times \gamma\left(k+1, \frac{\lambda_1 u}{\lambda_2(1-\rho)}\right) du \end{aligned} \tag{7}$$

where $\gamma(\cdot,\cdot)$ is the incomplete gamma function defined by [16]

$$\gamma(n+1,x) = n! - n! e^{-x} \sum_{m=0}^{n} \frac{x^m}{m!}$$

Further with some manipulations, R_k^1 can be rewritten as

$$\begin{aligned} R_k^1 &= \int_0^\infty k! (1-\rho)^{k+1} \ln(1+\lambda_1 u) \exp\left(-\frac{u}{1-\rho}\right) u^k du \\ &-k! \sum_{m=0}^{k} \frac{(\lambda_1/\lambda_2)^m}{m!} \int_0^\infty (1-\rho)^{k+1-m} \ln(1+\lambda_1 u) \\ &\times \exp\left(-\frac{1+\lambda_1/\lambda_2}{1-\rho} u\right) u^{k+m} du \end{aligned} \tag{8}$$

Using (6), we can evaluate the integral

$$\begin{aligned} R_k^1 &= k! (1-\rho)^{k+1} F\left(\lambda_1, k, \frac{1}{1-\rho}\right) \\ &-k! \sum_{m=0}^{k} \frac{(\lambda_1/\lambda_2)^m}{m!} (1-\rho)^{k+1-m} F\left(\lambda_1, k+m, \frac{\lambda_1/\lambda_2}{1-\rho}\right) \end{aligned} \tag{9}$$

Similarly, we evaluate R_k^2 by using the complementary incomplete gamma function $\Gamma(n+1,x) = n! e^{-x} \sum_{m=0}^{n} \frac{x^m}{m!}$ [16]. It yields

$$R_k^2 = k! \sum_{m=0}^{k} \frac{(\lambda_2/\lambda_1)^m}{m!} (1-\rho)^{k+1-m} F\left(\lambda_2, k+m, \frac{1+\lambda_2/\lambda_1}{1-\rho}\right) \tag{10}$$

■

B. outage probability of secrecy capacity

The secrecy capacity can also be characterized in terms of the outage probability for a target secrecy rate. The outage probability can be calculated according to

$$P_{out}(R) = 1 - P_r(C_s(\alpha,\beta) > R)$$
$$= 1 - P_r\left(\alpha > e^R(1+\beta) - 1\right)$$

Theorem 2: Similarly invoking again the infinite-series representation of $I_0(x)$, the outage probability is equivalent to

$$P_{out}(R) = 1 - \exp\left(-\frac{y}{1-\rho}\right)\sum_{k=0}^{\infty} c_k k! \sum_{m=0}^{k}\frac{1}{m!}\left(\frac{\mu}{1-\rho}\right)^m \times \sum_{n=0}^{m}\binom{n}{m}\left(\frac{y}{\mu}\right)^{m-n}\left(\frac{1-\rho}{1+\mu}\right)^{k+n+1}\Gamma(k+n+1) \tag{11}$$

where $y = \left(e^R - 1\right)/\lambda_1$ and $\mu = e^R\lambda_2/\lambda_1$.

At this point in this study, the closed-form expressions of secrecy capacity have been derived for a correlated Rayleigh fading channel. In all cases of practical significance, the infinite series representations can be truncated without sacrificing numerical accuracy. We also note that the results in [7] are a special case of our result by assuming independent channels.

IV. Simulation Results

In Fig. 2, we plot the secrecy capacity versus SNR over correlated fading channels in the case of the scenario that the SNR of main channel and eavesdropper's channel are equal.

It is clearly shown that the correlation between the main and the eavesdropper's channel reduce the secrecy capacity. For comparison, the limiting value given in [14] also is depicted in Fig 2. The secrecy capacity converges into the limit of the secrecy capacity [14] at high SNRs. However, the limiting value is far away form the secrecy capacity at low and moderate SNRs.

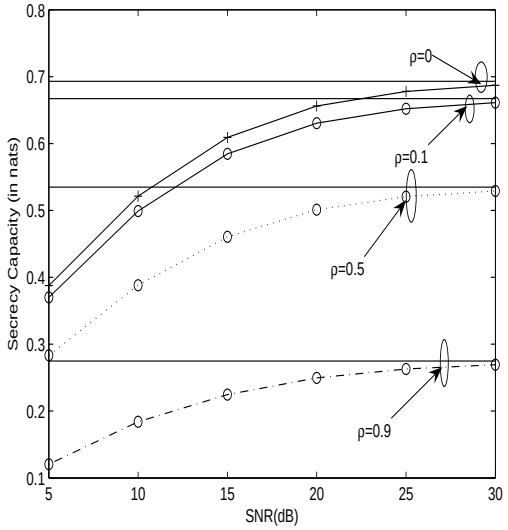

Fig. 2. The average secrecy capacity versus SNR over the correlated fading channels. The average SNR of main channel and eavesdropper's channel are equal. The solid lines indicates the limiting value given in [14].

V. Conclusion

In this paper, we investigate the secure communication over correlated Rayleigh fading Wyner's wiretap channel. The closed form expressions for average secrecy capacity and outage probability are derived assuming the full channel state information available.

Acknowledgment

This work is supported by National Science Foundation of China under Grant 60802007 and supported by the Research Fund of National Mobile Communications Research LaboratorySoutheast University 2009A10.

References

[1] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Info.Theory.*, vol.39, pp. 733-742, May. 1993.
[2] A. D.Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol.54, no.5, pp.1355-1367, Oct. 1975.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory.*, vol.24, no.3, pp. 339-348, May 1978.
[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory.*, vol.24, no.4, pp. 451-456, Jul 1978.
[5] Wei kang and Nan Liu, "The Secrecy Capacity of the Semi-deterministic Broadcast Channel," *in Proc. IEEE ISIT.*, Seoul, Korea, Jun. 2009, pp. 2767-2771.
[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *in Proc. IEEE ISIT.*, Seattle, WA, Jul. 2006, pp. 356-360.
[7] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues and Steven W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Info.Theory.*, vol.54, no.6, pp. 2515-2534, May 2008.
[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info.Theory.*, vol.54, no.10, pp. 4687-4698, Oct 2008.
[9] Z. Li, W. Trappe and R. Yates, "Secret communication via multiantenna transmission," *in Proc. 41st Conference on Information Sciences and Systems.*, Mar 2007.
[10] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *in Proc. IEEE ISIT.*, Jun 2007, pp. 2466 - 2470.
[11] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory.*, vol.54, no.9, pp. 4005 - 4019, Sept 2008.
[12] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," *in Proc. 46th Annual Allerton Conf. Commun., Control, and Computing.*, Sept 2008, pp.1132 - 1138.
[13] L. Dong, Z. Han, A. Petropulu and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *in Proc. IEEE ICASSP.*, Apr 2009, pp.2613 - 2616.
[14] H. jeon, N. Kim, M. Kim, H. Lee and J. Ha"Secrecy capacity over correlated ergodic fading channel," *in Proc. IEEE Military Comm.*, 2008.
[15] Marvin K. Simon, *Probability Distributions Involving Gaussian Random Variables.*, Springer Press, 2006.
[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products,6th ed.*, San Diego:CA, Academic press, 2000.